Signal jamming

Signal jamming is the deliberate transmission of strong radio signals to create interference, which overwhelms and obstructs targeted wireless communications such as Wi-Fi, cellular, and GPS. This intentional disruption of signals serves various purposes, including military applications to confuse enemy radar and communications, criminal use to block vehicle trackers or disrupt security systems, and government-sanctioned censorship. The core principle is to "drown out" a desired signal with a stronger, interfering one, rendering devices inoperable.

- How it Works:

* Frequency Detection:

A signal jammer first identifies the frequencies used by the target wireless devices.

* Signal Overpowering:

The jammer then broadcasts a powerful, noisy signal on those same frequencies.

* Signal-to-Noise Ratio Decrease:

This strong, interfering signal decreases the signal-to-noise ratio at the receiver, making it impossible for the intended device to receive the correct data and effectively "jamming" the communication channel.

- Uses and Applications:

* Military:

Used to confuse enemy radar, disrupt communications, and obscure target signals during electronic warfare.

* Security & Privacy:

Criminals use jammers to block GPS and cellular signals for vehicle tracking systems to evade capture, or to disrupt alarms during burglaries.

*** Censorship:**
Authoritarian regimes may use signal jamming to prevent citizens from receiving foreign broadcasts or accessing information.
*** Prisons:**
In some jurisdictions, signal jamming is specifically permitted within correctional facilities to block unauthorized communication.
- Legal Status:
The use, sale, and importation of signal jammers are often illegal due to their potential to interfere with essential services like emergency communications and critical infrastructure.
Impact
Signal jamming can lead to a temporary but complete denial of service for wireless devices in an area.
It poses risks to public safety by disrupting emergency response communications and can compromise security systems.

By: Haytham Zeidan

Resources:

https://www.britannica.com/topic/electronic-warfare

https://www.cartrack.co.za/blog/signal-jamming-detection-cartracks-advanced-technology-has-got-you-covered

https://acasom.com/blogs/news/understanding-what-is-a-signal-jammer-module

https://en.m.wikipedia.org/wiki/Radio_jamming

https://www.dhs.gov/news/2025/06/18/homeland-security-warns-about-spike-china-based-technology-firms-smuggling-signal

https://www.theiet.org/media/8779/jamming-and-radio-interference.pdf